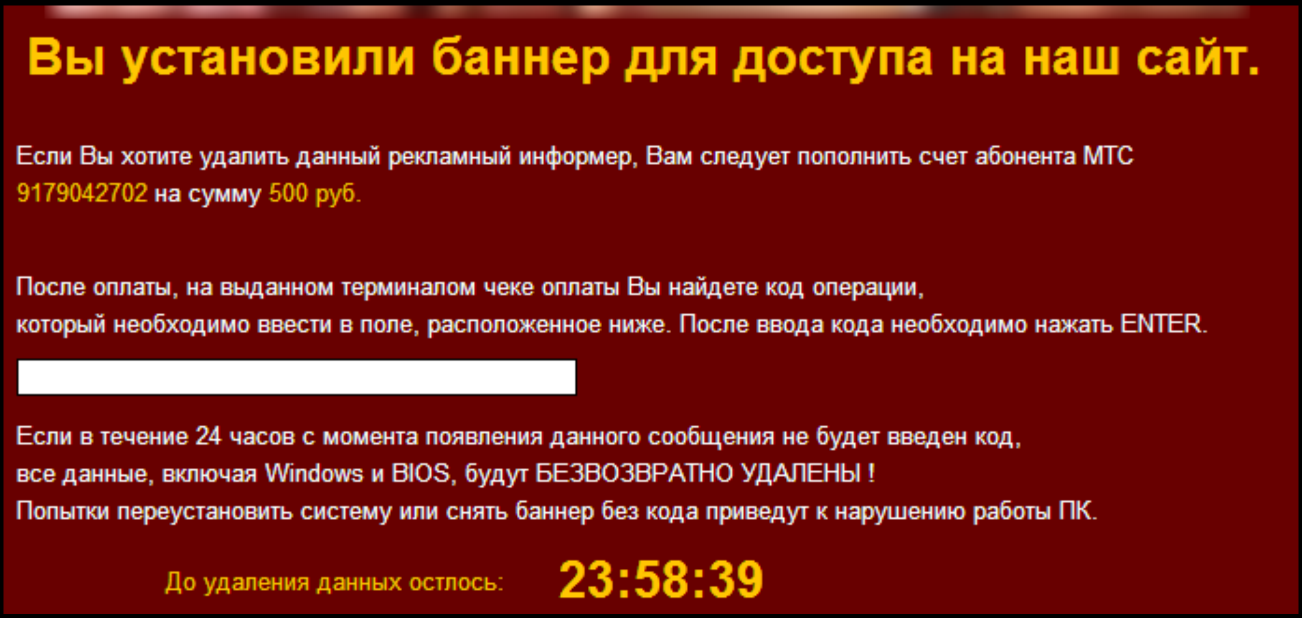
Low Tech Ransomware

In the information age in which we live the flow of data is everything. Interrupting or even worse holding data hostage can create great loss for individuals and businesses. It's not without surprise that cyber criminals recognize this dependency and have found ways of turning a profit by exploiting our dependency on our own data ... enter Ransomware. Ransomware, or ransom malware, first appeared in the late 80s (*1989 PC Cyborg Trojan*[1]). Even though ransomware has been around with an on again/off again showing it hasn't been until recent years that we have seen a steep increase in the volume and earning potential of this type of malware. The typical formula for this type of malware is to locate and encrypt user data and require the user to pay for the decryption. A number of industry standard and custom encryption algorithms have been used over the years to encrypt the data which has generated mix results in developing alternative (alternate to just paying the ransom) means for recovering the lost data. This history has created a semi-awareness in the industry that if infected you really have two primary options, restore from backup or pay the ransom.

Recently, I had the opportunity to analyze a ransomware sample. What I found was an interesting sample (*8dfa99320d7d301b6d35c2fbf98e5b7a*) that relied more on social engineering than on advanced tech to extort money from the end user. During sample analysis the first visual was a typical ransomware popup informing me that my data is now hostage and a ransom must be paid.



Вы установили баннер для доступа на наш сайт.

Если Вы хотите удалить данный рекламный информер, Вам следует пополнить счет абонента МТС 9179042702 на сумму 500 руб.

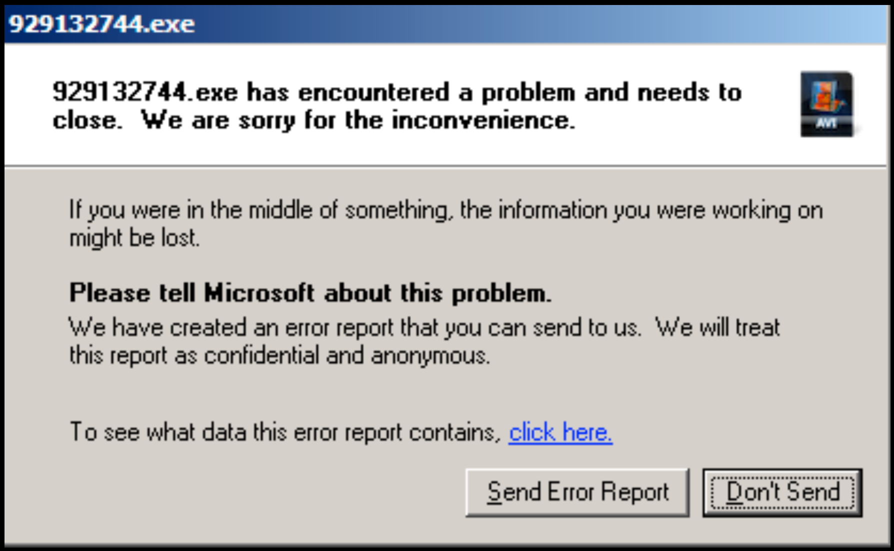
После оплаты, на выданном терминалом чеке оплаты Вы найдете код операции,
который необходимо ввести в поле, расположенное ниже. После ввода кода необходимо нажать ENTER.

Если в течение 24 часов с момента появления данного сообщения не будет введен код,
все данные, включая Windows и BIOS, будут БЕЗВОЗВРАТНО УДАЛЕНЫ !
Попытки переустановить систему или снять баннер без кода приведут к нарушению работы ПК.

До удаления данных остлось: 23:58:39

As is evident from the graphic, a Russian or Russian-speaking user is being targeted and 500 rubles (about $17) is the ransom price. Additionally, the user had 24 hours to meet the demands or else all data would be wiped. One slight twist to the typical ransom note was that a number of pornographic images were displayed across the top of the popup. This points to a probable delivery through porn sites, but I think this also has a social engineering benefit that could apply additional pressure on the user to pay the ransom. As you can imagine, if the user was interested in keeping an overt surfing habit a secret or perhaps the computer used was a work computer or family computer an end user may decide to just pay the ransom. If a user was still reluctant to pay, the ominous clock counting down from 24:00 hours with the threat of losing all data would generate additional pressure. To close the deal, the malware takes exclusive control of the keyboard and mouse and forces focus on the entry field of the ransom dialog with no ability to escape or close the window.

During the first pass of analysis, I discovered that the countdown was a hollow threat. First, the clock resets to 24:00 after each reboot. Next I discovered allowing the time to expire simply crashed the malware.



929132744.exe has encountered a problem and needs to close. We are sorry for the inconvenience.

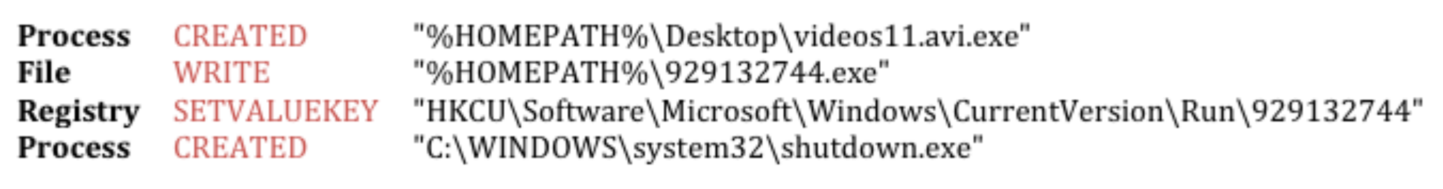
If you were in the middle of something, the information you were working on might be lost.

Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

After the malware crash, system control was returned to the end user and all was well until the next reboot.

Deeper system analysis revealed no files were encrypted! As a matter-of-fact the malware didn't even attempt to locate user files. Instead, the malware is a simple EXE (PE32) file that takes exclusive focus on the system once launched and persists using a simple auto start at boot registry key setting.



```
Process   CREATED      "%HOMEPATH%\Desktop\videos11.avi.exe"
File      WRITE        "%HOMEPATH%\929132744.exe"
Registry  SETVALUEKEY  "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\929132744"
Process   CREATED      "C:\WINDOWS\system32\shutdown.exe"
```

Killing the malware process returns the system to a normal state and removing the file and registry key stops the ability to persist at reboot. Obviously, there is no way to know how much money the attacker earned using this approach but my money is on the fact a perceived threat is just as lucrative as a real threat.

[1] *Aids (trojan horse)*. (2011, January 16). Retrieved from http://en.wikipedia.org/wiki/PC_Cyborg_Trojan